IN THE SPECIFICATION:

[0008] Instructions in accordance with various embodiments of the present invention can be stored on a medium, such as a hard disk, a CD-ROM (compact disc read only memory), a telecommunications channel (e.g., in transit over a network); flash memory; and anything that can store digital information.

[0010] Recipient 110 can include a processor 111 coupled to memory 112 that stores recipient instructions 113 that are adapted to be executed by processor 111 to perform at least a part of the method in accordance with an embodiment of the present invention. For example, recipient instructions 113 can receive from server 106 a message indicating that certain content from sender 101 is ready to be delivered to recipient 110. Recipient instructions 113 can provide a recipient GUI to a user at recipient 110 through which the recipient user can send a message to serve 106 to send the content to recipient 110. Recipient can also include various ancillary memory devices, such as storage media A 114, storage media B 115, and other storage media, e.g., including storage media Z 116. In one embodiment, storage media A is a flash memory device; storage media B is a CD (compact disc); storage media Z is a DVD (digital video disc); etc.

[0012] Consistent with the content policy, processing instructions 109 can be executed by processor 107 to determine if recipient has the appropriate recipient instructions 113 (e.g., has recipient instructions 113 at all, has a current version of recipient instructions 113, etc.). In this example, recipient instructions ~~119~~ 113 include software for writing data to a CD ("CD burning instructions"). If server 106 determines that recipient does not have the appropriate recipient instructions 113 installed, then server 106 can send (or arrange to have sent) the appropriate recipient instructions 113, which, in this embodiment, include CD burning instructions. When these have been successfully installed at recipient 110, server 106 can exchange messages with recipient 106 such that the content is sent from server 106 to recipient 110 and persistently installed only on a CD, i.e., on storage media B 115. Server can ensure that no other persistent copy of the content is stored elsewhere by sending the appropriate data and/or instructions to recipient processor 111, which is executing recipient instructions 113. For example, if no CD is present at recipient 110, or if no CD burning instructions are installed at recipient 110, then server 106 can refuse to send the content to recipient 110. In this way, sender 106 can advantageously control the medium onto which content sent from sender 101 to recipient 110 (through server 106) is persistently stored.

[0013] Server 106 can also provide Digital Rights Management (DRM) services by handling content from sender 101 consistently with a content policy. DRM includes technical measures for controlling the distribution, redistribution, storage and/or use of content. For example, server 106 can obtain content from sender 101 over a Secure Sockets Layer (SSL) connection, i.e., the content can be encrypted using a set of symmetric keys shared for a session between sender 101 and server 106. Sender instructions 104 can provide a user friendly GUI to a user at sender 101 through which the sender-user can specify one or more DRM parameters that control the content. For example, as discussed above, the sender-user can specify through the GUI that the content be delivered to recipient and persistently stored only on a CD. Server 106 can enforce this sender-set policy by ensuring that the appropriate CD burning instructions are installed at recipient 110 and an appropriate (e.g., blank) CD is present at recipient 110 before sending the content to recipient 110. Server 106 can then interact with recipient 110 to ensure that the content is properly installed (persistently stored) on the CD, and nowhere else. For example, server 106 can utilize controls such as those proposed for computer systems by the Trusted Computing Platform Alliance (TCPA)~~, see <http://www.trustedcomputing.org>,~~ and the Palladium system developed by the Microsoft Corporation of Redmond, Washington~~, see < http://www.microsoft.com/presspass/features/2002/jul02/0724palladiumwp.asp>.~~ The TCPA and Palladium controls help to provide assurance that a computing platform operates in a trusted fashion, i.e., that is protects the confidentiality and integrity of content in accordance with policies set forth by the rights holders in and to the content. These policies can be implemented in software and/or hardware. The measures set forth in accordance with TCPA and Palladium requirements and/or specifications help to ensure that the software and/or hardware of a computing platform implements the policies correctly, completely and exactly. The software used in an embodiment of the present invention to implement the policies can include recipient instructions 113; processing instructions 109; and sender instructions 104.

[0019] In accordance with an embodiment of the present invention, a first user, User A, can send content to a second user, User B, and mandate that the content be stored on a CD at User B. User A and User B can be connected to the Internet via broadband connections, and User B can have a CD-RW (compact disc rewritable) drive in his computer. The users' computers can both be behind router/firewalls which perform network address translation (NAT) and block incoming traffic. Assume that neither user has yet used the present invention.

[0027] The web page can also download a recipient software auto-installer if needed. The auto-installer can install the recipient software, which can then be launched. The recipient software can prompt User B to enter the required data to complete his account registration. The recipient software can then scan User B's system for a CD-R/RW (compact disc recordable/rewritable) device. If it finds more than one such a device, it can prompt the User B to specify at which one he wants the package to be stored. User B can decide to receive the package immediately or he can defer this for another time. If he elects to pick up the package, the client software can contact the server and download the package. As with the upload, status can be displayed on the progress of each step, and the recipient software GUI can advantageously be minimized/hidden to work in the background. When the package is downloaded, the recipient software can decode the content. The recipient software can check for a suitable blank disc in the recipient's CD-R/RW drive, and instructs User B to insert one if needed. The content can then be stored on the CD. Once the CD-R/RW has been written, the client determines if the write was successful. If so, it can inform User B and report to the server that the package has been delivered. The server can then send a message to User A to inform him that the package has been received by User B.

[0037] Figure 3 shows examples of selections ~~302~~ on GUI 300 that can be made by the sending user to impose digital rights management controls on the content to be transferred. As discussed above and as shown ~~in 302~~, the sending user can require that the recipient user be able to make no copies from the recipient's copy of the transferred content; specify a maximum permissible number of such copies; a maximum number of outstanding copies; a maximum number of times a copy may be used; a fee amount based upon use of the copy or copies; and a credit amount based upon the use of the copy or copies. Any or all of these parameters, as well as any other suitable parameter, can also be set by server 106. For example, server 106 can implement a policy that requires a maximum permissible number of copies for content that includes a given company (e.g., ACME Music Company) among its rights holders. The policies of the server 106 can be made to preempt designations made by the sending user. Thus, if the sending user specifies that a given piece of content to be transferred from the sender 101 to the recipient through server 106 is six, and if a preempting policy at the server 106 mandates at most 4 copies, then processing instructions 109 at the server 106 can overwrite the transfer parameter set by the sending user (six) with its own parameter (four). As above, such a transfer parameter can be used by recipient instructions 113 to enforce a digital rights management rule for the transferred content at the recipient 110. Likewise, server 106 policies can be preempted by sending user policies.

[0040] A recipient memory device can be discovered and specified to the sending user in any suitable way. For example, as shown in Figure 4, the recipient memory device can be specified by a device identifier; type (e.g., hard disk, flash memory, writeable CD-ROM, etc.); user name (e.g., the recipient user; the owner of the memory device; etc.); organization identifier (e.g., manufacturer's name; company-owner name; etc.); model identifier; capability (e.g., DRM-enabled, capacity (e.g., in megabytes); speed (the rates at which data may be transferred to and/or from the device); bus compatibility (e.g., USB (universal serial bus), PCI (peripheral component interconnect), SCSI (small computer system interface), etc.); or any other criterion or criteria that can be useful in designating a recipient memory device for receiving content from the sender. A recipient memory device criterion can be any property of a recipient memory device that can be required to store on that device one or more pieces of electronic content from a sender. If the sending user specifies that only a memory device having the identifier 14534 may store a given item of electronic content from the sender, then the recipient memory device must have that criterion (identifier 14534) to store the sent content. If no such memory device having the specified criterion or criteria exists at a recipient, then the sender can refuse to send the content to the recipient.